

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-216045

(43)Date of publication of application : 10.08.2001

(51)Int.Cl G06F 1/00
G06F 15/00
H04L 9/32

(21)Application number : 2000-025816 (71)Applicant : NEC CORP

(22)Date of filing : 03.02.2000 (72)Inventor : UCHIDA KAORU

(54) BIOMETRICS INPUTTING DEVICE AND BIOMETRICS COLLATING DEVICE

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a biometrics inputting device capable of surely verifying a person himself or herself without generating any security hole even when biometrics inputting part and processing part are not necessarily integrated. SOLUTION: A fingerprint sensor 11 photographs a fingerprint picture when a finger is touched and converts the photographed input picture into digital data and transmits it to a picture enciphering part 13. The picture enciphering part 13 enciphers the input picture based on an encipherment key from an encipherment key holding part 12. A picture decoding part 21 decodes the signal received from the fingerprint inputted device 1 by using the key from the encipherment information holding part 24. A fingerprint feature extracting part 22 calculated features to be used for fingerprint collation from the picture information being the decoded result. A fingerprint feature collating part 23 collates the fingerprint features obtained by the fingerprint feature extracting part 22 with the fingerprint features of a user registered for an each user fingerprint registration information table 26 and transfers the result to a collated result judging part 25.

CLAIMS

[Claim(s)]

[Claim 1] A biometrics inputting device comprising:

A sensor means which digitizes biometrics which is the living body feature peculiar to an individual.

Confidential information holding mechanism holding an enciphering key which is the confidential information set up beforehand.

A biometrics encoding means which enciphers and outputs biometrics digitized by said sensor means based on an enciphering key held at said confidential information holding mechanism.

[Claim 2]The biometrics inputting device according to claim 1 constituting said sensor meanssaid confidential information holding mechanismand said biometrics encoding means as an indivisible portion.

[Claim 3]The biometrics inputting device according to claim 1 or 2 using a fingerprint as said biometrics.

[Claim 4]A biometrics inputting device comprising:

A sensor means which digitizes biometrics which is the living body feature peculiar to an individual.

Confidential information holding mechanism holding an enciphering key which is the confidential information set up beforehand.

A digital-watermarking encoder which embeds an enciphering key held at said confidential information holding mechanism at biometrics digitized by said sensor means as digital watermarking.

[Claim 5]The biometrics inputting device according to claim 4 constituting said sensor meanssaid confidential information holding mechanismand said biometrics encoding means as an indivisible portion.

[Claim 6]The biometrics inputting device according to claim 4 or 5 using a fingerprint as said biometrics.

[Claim 7]Holding mechanism holding an enciphering key which is the confidential information beforehand set up for every biometrics inputting deviceA decoding means which decrypts the biometrics concerned using an enciphering key peculiar to said biometrics inputting device held at said holding mechanism at the time of an input of biometrics enciphered based on said enciphering keyA biometrics collating unit having a collation processing means to perform collation processing of said biometrics decrypted by said decoding means.

[Claim 8]The biometrics collating unit according to claim 7 using a fingerprint as said biometrics.

[Claim 9]A decoding means which decrypts the biometrics concerned using an enciphering key peculiar to said biometrics inputting device which came to hand separately at the time of an input of biometrics enciphered based on an enciphering key which is the confidential information beforehand set up for every biometrics inputting deviceA biometrics collating unit having a collation processing means to perform collation processing of said biometrics decrypted by said decoding means.

[Claim 10]The biometrics collating unit according to claim 9 using a fingerprint as said

biometrics.

[Claim 11] A biometrics collating unit comprising:

Holding mechanism holding an enciphering key which is the confidential information beforehand set up for every biometrics inputting device.

A means which takes out said enciphering key from the biometrics concerned at the time of an input of biometrics where said enciphering key was embedded as digital watermarking.

A means to compare said the taken-out enciphering key with an enciphering key held at said holding mechanism and to judge the justification of a signal from said biometrics inputting device.

A collation processing means to perform collation processing of said biometrics using the decision result.

[Claim 12] The biometrics collating unit according to claim 11 using a fingerprint as said biometrics.

[Claim 13] A biometrics collating unit comprising:

A means which takes out said enciphering key from the biometrics concerned at the time of an input of biometrics where an enciphering key which is the confidential information beforehand set up for every biometrics inputting device was embedded as digital watermarking.

A means to compare said the taken-out enciphering key with confidential information peculiar to said biometrics inputting device which came to hand separately and to judge the justification of a signal from said biometrics inputting device.

A collation processing means to perform collation processing of said biometrics using the decision result.

[Claim 14] The biometrics collating unit according to claim 13 using a fingerprint as said biometrics.

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Field of the Invention] Especially this invention relates to the biometrics inputting device and biometrics collating unit for the user authentication in an information security etc. and identification about a biometrics inputting device and a biometrics collating unit.

[0002]

[Description of the Prior Art] In the information service which leads the electronization and the network of information for reservation of the security which opposes the

injustice and crime of tapping and an alteration and "spoofing" of data. Realization of personal identification for the partner of whether human being who accesses information is a user with just authority and exchange of value to check whether you are a user whom he desires serves as indispensable conditions.

[0003] Although the magnetic card and the password are used for personal identification now. For example, when a card is lost or you forget a password in any case, there is a problem that others become and clear up easily by a theft and forgery or a furtive glance and a guess as well as there being inconvenient [that the person himself/herself cannot use either].

[0004] Then the biometrics which solves these problems is used. The living body feature peculiar to an individual [like a fingerprint] whose biometrics is used. It is supposed that the fingerprint which is a pattern of dermatoglyphic of human being's fingertip has the feature - "permanent throughout the life" "unique throughout the world" and since the same fingerprint is restored from the eternal dermis of the back even if epidermis receives damage it is widely known as biometrics which enables a precise individual's identification.

[0005] A "biometrics inputting device" with which the system which attests an individual by biometrics acquires fundamentally the biometrics which the user presented by the system side. The "feature extraction part" which searches for the feature which processes the inputted data and is used for collation. It comprises "collation and a judgment part" which compares with registration data and input data (the features) the registration data ("template") about the registered user who asks beforehand and memorizes and determines whether be the same person.

[0006] The feature is similar enough as a result of collation and if judged with the presentation person of biometrics being a registered user, the authentication demand person can receive the service to demand by an authentication success. Hereafter a fingerprint is mentioned and explained as an example of biometrics.

[0007] In order to acquire an optical system especially a high contrast picture conventionally as an input device of a fingerprint, only the method of using the total internal reflection in prism has been used. After this applies the light emitted with the LED (Light Emitting Diode) light source to prism, a photo detector like CCD (Charge Coupled Device) receives it. Unevenness of the finger put on the reflector of prism is made to reflect in the difference in reflectance and is digital-image-ized.

[0008] The unevenness is sensed in recent years as an element which makes sensing other than an optical system possible from the fingerprint which carried out direct contact on the surface of the semiconductor chip. For example, the thing of a capacitive sensing method, the thing of the method which detects temperature and the difference of an electric field etc. are being put in practical use.

[0009]

[Problem(s) to be Solved by the Invention] The method of an input device performing only the input of a fingerprint and carrying out as a realization method of fingerprint

authentication processing by the server etc. which were connected with PC (personal computer) to which identification processing was connected or the network may be taken.

[0010] Thus when the fingerprint input device (scanner) and the collation processing section have dissociated an input device (called an input scanner and an input sensor) inputs a fingerprint image it is sent to PC through a cable etc. and feature extraction and collation and decision processing are performed there.

[0011] A cable is changed other information machines and equipment are tied with such composition and there may be a security attack of inputting into a collation processing section the image data of others' fingerprint which came to hand at other opportunities [an input sensor]. In this case although the fingerprint of the person himself/herself who demands service is considered and service is permitted in a collation processing section it may happen that it was others' fingerprint actually.

[0012] Then without producing a security hole even when the purpose of this invention cancels the above-mentioned problem and the biometrics input part and the treating part are not necessarily unifying it is in providing the biometrics inputting device and biometrics collating unit which can perform positive personal identification.

[0013]

[Means for Solving the Problem] A biometrics inputting device by this invention is provided with the following.

A sensor means which digitizes biometrics which is the living body feature peculiar to an individual.

Confidential information holding mechanism holding an enciphering key which is the confidential information set up beforehand.

A biometrics encoding means which enciphers and outputs biometrics digitized by said sensor means based on an enciphering key held at said confidential information holding mechanism.

[0014] Other biometrics inputting devices by this invention are provided with the following.

A sensor means which digitizes biometrics which is the living body feature peculiar to an individual.

Confidential information holding mechanism holding an enciphering key which is the confidential information set up beforehand.

A digital-watermarking encoder which embeds an enciphering key held at said confidential information holding mechanism at biometrics digitized by said sensor means as digital watermarking.

[0015] A biometrics collating unit by this invention is provided with the following.

Holding mechanism holding an enciphering key which is the confidential information beforehand set up for every biometrics inputting device.

A decoding means which decrypts the biometrics concerned using an enciphering key peculiar to said biometrics inputting device held at said holding mechanism at the time of an input of biometrics enciphered based on said enciphering key.

A collation processing means to perform collation processing of said biometrics decrypted by said decoding means.

[0016]Other biometrics collating units by this invention are provided with the following.

A decoding means which decrypts the biometrics concerned using an enciphering key peculiar to said biometrics inputting device which came to hand separately at the time of an input of biometrics enciphered based on an enciphering key which is the confidential information beforehand set up for every biometrics inputting device.

A collation processing means to perform collation processing of said biometrics decrypted by said decoding means.

[0017]Another biometrics collating unit by this invention is provided with the following.

Holding mechanism holding an enciphering key which is the confidential information beforehand set up for every biometrics inputting device.

A means which takes out said enciphering key from the biometrics concerned at the time of an input of biometrics where said enciphering key was embedded as digital watermarking.

A means to compare said the taken-out enciphering key with an enciphering key held at said holding mechanism and to judge the justification of a signal from said biometrics inputting device.

A collation processing means to perform collation processing of said biometrics using the decision result.

[0018]Furthermore it is based on this invention another biometrics collating unit is provided with the following.

A means which takes out said enciphering key from the biometrics concerned at the time of an input of biometrics where an enciphering key which is the confidential information beforehand set up for every biometrics inputting device was embedded as digital watermarking.

A means to compare said the taken-out enciphering key with confidential information peculiar to said biometrics inputting device which came to hand separately and to judge the justification of a signal from said biometrics inputting device.

A collation processing means to perform collation processing of said biometrics using the decision result.

[0019]That is a biometrics inputting device of this invention is enciphering biometrics data acquired with an input device with a key peculiar to an input device or embedding data peculiar to an input device as digital watermarking and enables a check of the

justification of a biometrics inputting device by the collating-unit side.

[0020] Since it becomes possible to detect it when a biometrics inputting device is converted and replaced by this or an output signal is replaced, it becomes possible to perform positive personal identification without producing a security hole even when a biometrics input part and a treating part are not necessarily unifying.

[0021]

[Embodiment of the Invention] Next, working example of this invention is described with reference to Drawings. Drawing 1 is a block diagram showing the composition of the biometrics inputting device by one working example of this invention. An example of the composition in the case of logging in a user with a fingerprint in PC etc. in drawing 1 is shown. The fingerprint input device 1 is connected to PC by local connection of a cable etc. and the fingerprint collating part 2 operates by the software on PC.

[0022] The fingerprint input device 1 is equipped with the fingerprint sensor 11 and when a user's finger contacts after the fingerprint sensor 11 photos the fingerprint image and changes the photoed inputted image into digital data, it is sent to the picture enciphering part 13. The enciphering key attaching part 12 holds the enciphering key peculiar to the individual of the fingerprint input device 1 as confidential information which is not known by the general user etc. This is a 256-bit bit string etc. for example.

[0023] The picture enciphering part 13 receives the enciphering key from the enciphering key attaching part 12 and performs encryption processing of an inputted image by making this into a key. Although the encryption method of a common secret key method which makes DES (Data Encryption Standard) an example can be used as this encryption processing, it is also possible to use the cipher system of a public key system (asymmetric cipher system) which makes a RSA method an example on the other hand. In this case, the secret key which the fingerprint input device 1 has will be used for encryption.

[0024] The method of adopting the scramble processing shifted or replaced for every line of an inputted image or pixel depending on a use even if it is not complicated encryption processing and putting on the enciphering key attaching part 12 by using as an enciphering key the rule which specifies the scramble is also possible.

[0025] On the other hand, it is desirable to constitute the fingerprint sensor 11, the picture enciphering part 13 and the enciphering key attaching part 12 from an indivisible method as construction of the fingerprint input device 1. The unjust third party who aims at a decipherment and reconstruction of the portion here as it is indivisible, Decode the internal signal from the fingerprint sensor 11 to the picture enciphering part 13 and the internal signal from the enciphering key attaching part 12 to the picture enciphering part 13 or I hear that it constitutes so that those signals may be replaced by the signal from the outside, the contents of each component may be decoded or it cannot convert and it is.

[0026] The method of burning the picture enciphering part 13 and the enciphering key

attaching part 12 is effective on the chip same as this real overseas subsidiary as the semiconductor chip which performs image acquisition of the fingerprint sensor 11 and digitization. As an example the imager chip of CMOS (Complementary Metal Oxide Semiconductor) is used as an image pick-up part of the fingerprint sensor 11. There may be mounting of performing from maintenance of an encryption key to encipherment arithmetic on the same chip and making the enciphered result into an output signal.

[0027] Or fingerprint sensing of the capacitive sensing method by a semiconductor sensor can be used as a fingerprint image acquisition method of the fingerprint sensor 11 and it can also be said that from maintenance of an encryption key to encipherment arithmetic is mounted on the semiconductor sensor.

[0028] In the fingerprint collating part 2 connected to the fingerprint input device 1 by local connection of a cable etc. to the encipherment information attaching part 24 of the inside. For every individual of the fingerprint input device 1 which the fingerprint collating part 2 connects and uses a peculiar enciphering key is made into the identifier (device ID) of the input device and a pair and is memorized and the key corresponding to device ID of the fingerprint input device 1 which should be connected now is passed to the fingerprint decoding section 21. The image decoding part 21 decodes the signal received from the fingerprint input device 1 using the key.

[0029] It has that this decoding processing can restore the right meaningful signal using the thing corresponding to the contents of processing of the picture enciphering part 13 of the fingerprint input device 1 and the justification of the signal sent from the fingerprint input device 1 and there is checked -- things -- **

[0030] For example if the picture enciphering part 13 uses the encryption method of the common secret key method When decoding using the same key as what was held at the enciphering key attaching part 12 is performed and it can decode correctly now it can check that the signal sent from the fingerprint input device 1 and there is just.

[0031] If it is a cipher system of a public key system (asymmetric cipher system) it will decode using the public key corresponding to the secret key held at the enciphering key attaching part 12 of the fingerprint input device 1. When it can decode correctly now it can check that the signal sent from the fingerprint input device 1 and there is just.

[0032] The picture enciphering part 13 shifts for every line of an inputted image or pixel or Also when the scramble processing to replace is used it holds to the encipherment information attaching part 24 by using as a key the rule which specifies the scramble which the enciphering key attaching part 12 should have and decryption corresponding using it is performed. When it can decode correctly now it can check that the signal sent from the fingerprint input device 1 and there is just.

[0033] The fingerprint feature extraction part 22 calculates the feature used for fingerprint authentication from the picture information of the result decoded by the

image decoding part 21. The fingerprint registration information table 26 classified by user holds the fingerprint feature information used for fingerprint authentication for every user. The fingerprint feature collating part 23 performs collation with the fingerprint feature searched for by the fingerprint feature extraction part 22 and a user's fingerprint feature registered into the fingerprint registration information table 26 classified by user and passes a result to the collation result determining part 25.

[0034] As an example of realization of the fingerprint collation device containing the above fingerprint sensor 11 the fingerprint feature appearance part 22 and the fingerprint feature collating part 23 there is "fingerprint collation device" indicated to JPS56-24675A or JPH4-33065A.

[0035] In the "fingerprint collation device" indicated to JPS56-24675A. The local coordinates system determined by each focus peculiar with the positions X and Y and the direction D of each focus by which a fingerprint pattern is characterized when comparing a fingerprint etc. these days in the neighborhood divided into two or more sectorial regions The ridge count of a dot and the above-mentioned focus That is by inspecting relation high-precision collation is enabled stably.

[0036] In the "fingerprint collation device" indicated to JPH4-33065A it is supposed that it participates in neither the theft of a password nor oblivion and that operativity is excellent and it is possible in reliable identification by performing collation with one finger or two or more fingers of all and the input fingerprint which are registered.

[0037] The collation result determining part 25 synthesizes the justification of the signal sent from the fingerprint input device 1 and the result of the fingerprint authentication called for by the fingerprint feature collating part 23 and outputs them as a result of personal identification. It searches for the key information which must be [that the fingerprint collating part 2 is peculiar to the fingerprint input device 1 which should be used as stated previously and] secret from the table of the encipherment information attaching part 24 the signal sent from the fingerprint input device 1 using it is decoded and it checks whether it is the right meaningful signal.

[0038] When it means having agreed in the form of the signal outputted from the fingerprint sensor 11 in the right meaningful signal i.e. a fingerprint input device and this has agreed the fingerprint input device 1 is just It is judged that a fingerprint collated result is a reliable thing noting that it is able to check that the signal from the fingerprint input device 1 is not changed on the way.

[0039] Since it on the other hand means that didn't it have the just fingerprint input device 1 or the signal from the fingerprint input device 1 was changed on the way when it is not able to decode [agree] correctly it will be judged that a fingerprint collated result is not a reliable thing.

[0040] Drawing 2 is a block diagram showing the composition of the picture input device by other working example of this invention. In drawing 2 an example of the composition in the case of logging in a user with a fingerprint in PC etc. is shown like one working example of this invention the fingerprint input device 3 is connected to

PC by local connection of a cable etc. and the fingerprint collating part 4 operates by the software on PC.

[0041] The fingerprint input device 3 is equipped with the fingerprint sensor 11 and when a user's finger contacts after the fingerprint sensor 11 photos the fingerprint image and changes the photoed inputted image into digital data it is sent to the digital-watermarking encoder 31. The fingerprint input device confidential information attaching part 33 holds confidential information peculiar to the individual of the fingerprint input device 3 as confidential information which is not known by the general user etc. This is a character string like a password etc. for example.

[0042] The digital-watermarking encoder 31 receives the confidential information from the fingerprint input device confidential information attaching part 33 and embeds this with a digital-watermarking encoding method at an inputted image. With electronic watermark technology it has the following features.

[0043]. Namely (1) watermark data can be embedded in the invisible state into contents. (2) It has the feature that it is difficult for a third party to remove digital watermarking with the utility value of (4) contents which they can remain even if (3) watermarks which can be extracted when those who embedded the watermark are required process contents and can be extracted maintained. (2) sets up information like the key in encoding technology and if it does not use a key it is performed by establishing the structure which cannot take out information.

[0044] Without degrading the fingerprint image which is contents by using the above-mentioned electronic watermark technology electronic watermark data can be embedded into it and the data can be kept secret. Without degrading a fingerprint image substantially can separate and delete watermark data and it cannot be changed either. As an example of the real overseas subsidiary of electronic watermark technology for example among JPH8-241403A are the method of a description art given in JPH10-2247933A etc.

[0045] By the method of a description to JPH8-241403A. Although the pixel of a watermark picture can be inspected and the contents of the picture can be clearly seen by correcting the pixel to which a current image corresponds by changing the not a chromaticity but luminosity about each of the pixel which is not the "transparency" value as which the value was specified He is trying to bring about the visible mark which considers unapproved use of a picture and in which it is stopped.

[0046] With the art of a description to JPH10-2247933A. Management of the electronic watermark data to insert is simplified with outputting the electronic watermark data inserted with the MPEG (Moving Picture Experts Group) stream in which digital watermarking was inserted.

[0047] As construction of the above-mentioned fingerprint input device 3 it is desirable like one working example of this invention to constitute the fingerprint sensor 11 the fingerprint input device confidential information attaching part 33 and the digital-watermarking encoder 31 from an indivisible method. Since the output signal of the

digital-watermarking encoder 31 is included in the form in which a user's fingerprint image data appears as it is in the cryptopart 32 encryption processing is performed for communication content secrecy. Cipher systems such as a secret common key system etc. of DES usually used often may be sufficient as this and it should just be sharing the decoding part 41 and key information which are described below.

[0048] In the fingerprint collating part 4 connected to the fingerprint input device 3 by local connection of a cable etc. in the decoding part 41 the encryption for communication content secrecy is solved first and the output signal of the digital-watermarking encoder 31 is restored. Then in the digital-watermarking decoder 42 decoding (decryption) processing corresponding to the method of encoding of the digital-watermarking encoder 31 is performed and the watermark data embedded there is separated and detected from a fingerprint image signal.

[0049] The fingerprint input device 3 sends ID (identifier) peculiar to the device to the fingerprint collating part 4 apart from a fingerprint image signal. In the fingerprint collating part 4 confidential information corresponding to the individual of the fingerprint input device 3 which the fingerprint collating part 4 connects and uses for the fingerprint input device ID attaching part 43 of the inside is made into the identifier (device ID) of the input device and a pair and is memorized. This confidential information is the same as that of the information currently held at the fingerprint input device confidential information attaching part 33 of the applicable fingerprint input device.

[0050] The fingerprint input device ID attaching part 43 pulls this table by ID received from the fingerprint input device 3 reads corresponding confidential information and passes it to the fingerprint input device ID comparison part 44. The fingerprint input device ID comparison part 44 compares the value with the watermark data detected in the digital-watermarking decoder 42. If the fingerprint input device 3 is just these must be in agreement otherwise will become inharmonious.

[0051] The fingerprint feature extraction part 22 calculates the feature used for fingerprint authentication from the picture information outputted from the digital-watermarking decoder 42. The fingerprint registration information table 26 classified by user holds the fingerprint feature information used for fingerprint authentication for every user. The fingerprint feature collating part 23 performs collation with the fingerprint feature searched for by the fingerprint feature extraction part 22 and the fingerprint feature registered into the fingerprint registration information table 26 classified by user and passes a result to the collation result determining part 25.

[0052] The collation result determining part 25 synthesizes the justification of the fingerprint input device 3 which the fingerprint input device ID comparison part 44 judges and the result of the fingerprint authentication called for by the fingerprint feature collating part 23 and outputs them as a result of personal identification. If the information which must be [that the fingerprint collating part 4 is peculiar to the fingerprint input device 3 which should be used and] secret is embedded as digital

watermarking as stated previously the fingerprint input device 3 is just it is judged that it is what can trust a fingerprint collated result noting that it is able to check that the signal from the fingerprint input device 3 is not changed on the way.

[0053] Since it means that didn't it have the just fingerprint input device 3 or the signal from the fingerprint input device 3 was changed on the way when that is not right it will be judged that it is not what can trust a fingerprint collated result.

[0054] Drawing 3 is a block diagram showing the composition of the picture input device by another working example of this invention. In drawing 3 the picture input device by other working example of this invention is extended to the fingerprint authentication connected with the network.

[0055] The fingerprint input device 5 is connected to the service client 7 which a user uses. The POS (Point Of Sales) terminal for the public at the shop front of PC on the desk of a user's office PC at a user's home or a store etc. may be sufficient as this. Although these service clients work as a providing terminal of various information services or Electronic Commerce Technology Division to the user who is a customer about the personal identification and attestation of a user it functions as a transparent fixer who mediates between communication with the fingerprint server 6 and the fingerprint input device 5 without changing contents.

[0056] The fingerprint input device 5 connected to the service client 7 has the same composition as other working example of this invention and performs same operation. The fingerprint input picture where digital watermarking was embedded passes the service client 7 and is sent to the fingerprint server 6.

[0057] The fingerprint server 6 connected to the service client 7 by the network has the same composition as other working example of this invention fundamentally and performs same operation. That is digital watermarking is detected the justification of the fingerprint input device 5 judged by this and the result of the fingerprint authentication called for by the fingerprint feature collating part 23 are synthesized and it outputs as a result of personal identification.

[0058] However unlike the case of other working example of this invention the public-key-encryption part 51 enciphers the confidential information held independently at the fingerprint input device confidential information attaching part 33 using the public key of the RSA method corresponding to the fingerprint server 6 and a fingerprint image signal sends the fingerprint input device 5 to the fingerprint server 6.

[0059] In the secret key decoding part 61 the sent signal is decoded with the secret key corresponding to its public key and is used for comparison in the fingerprint input device ID comparison part 44. The confidential information enciphered using the public key of the RSA method corresponding to the fingerprint server 6 can be decoded only with the secret key corresponding to the public key.

[0060] Although the real overseas subsidiary that the fingerprint server 6 holds beforehand the pair of the confidential information and the fingerprint input device 5 corresponding to all the fingerprint input devices 5 tied in the network according to

other working example of this invention about this portion to that inside is also possible of course. In order for the number of the fingerprint input devices 5 to increase and to correspond to change exchange etc. it can be said that the direction to which confidential information is sent directly is excellent in another channel in this way.

[0061] The fingerprint server 6 tells the service client 7 about the output of the collation result determining part 25. Restricting to the time when it has checked from the result of the judgment if the user who inputted the fingerprint is a regular user and the fingerprint input device 5 is a regular device, the service client 7 provides the service which a user demands to the user.

[0062] Although explanation of working example of above-mentioned this invention mentions and explains the case of a fingerprint as an example of biometrics, if a means to input another biometrics for the portions of the fingerprint feature extraction part 22 and the fingerprint feature collating part 23 as the fingerprint sensor 11 and to extract and compare the feature replaces it, it is also possible to use other biometrics such as palm print, a face, the iris, a vascular pattern, a palm geometry, a hand, and a voiceprint. For example, in the case of a voiceprint, the justification of an input part can be checked by being inputted with a microphone and giving embedding of encryption or digital watermarking with a device indivisible from a microphone to Ushiro's digitized voice data.

[0063] Thus, by using for communication between a biometrics inputting device and a collating unit a signal undecipherable other than a collating unit or the signal which cannot decode and change digital watermarking embedded into it, a biometrics inputting device not being converted and replaced but judging that it is just -- the person himself/herself -- attestation can be performed.

[0064] A biometrics inputting device is connected with a collating unit in a cable or a network etc. by this. Even when having dissociated a cable, it can be changed. Other information machines and equipment can be tied and the security attack of the kind of inputting into a collation processing section the image data of others' fingerprint which came to hand at other opportunities [an input sensor] can be prevented. That is, although the fingerprint of the person himself/herself who demands service is considered and service is permitted in a collation processing section, it cannot happen that it was others' fingerprint in practice.

[0065] That is, when are replaced with the fingerprint data from the incongruent scanner with which data is not registered and operation is added to some data, you can detect them when a part is lost and can make it reflected in an authentication result.

[0066] Also when many biometrics inputting devices are on a network by taking the composition of another working example of this invention, user authentication can be realized checking that each is just.

[0067]

[Effect of the Invention] As explained above, according to this invention, the biometrics which is the living body feature peculiar to an individual is digitized. By enciphering and

outputting the digitized biometrics based on the enciphering key which is the confidential information set up beforehand. It is effective in the ability to perform positive personal identification without producing a security hole even when the biometrics input part and the treating part are not necessarily unifying.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1] It is a block diagram showing the composition of the biometrics inputting device by one working example of this invention.

[Drawing 2] It is a block diagram showing the composition of the biometrics inputting device by other working example of this invention.

[Drawing 3] It is a block diagram showing the composition of the biometrics inputting device by another working example of this invention.

[Description of Notations]

13 and 5 Fingerprint input device

2 and 4 Fingerprint collating part

6 Fingerprint server

7 Service client

11 Fingerprint sensor

12 Enciphering key attaching part

13 Picture enciphering part

21 Image decoding part

22 Fingerprint feature extraction part

23 Fingerprint feature collating part

24 Encipherment information attaching part

25 Collation result determining part

26 The fingerprint registration information table classified by user

31 Digital-watermarking encoder

32 Cryptopart

33 Fingerprint input device confidential information attaching part

41 Decoding part

42 Digital-watermarking decoder

43 Fingerprint input device ID attaching part

44 Fingerprint input device ID comparison part

51 Public-key-encryption part

61 Secret key decoding part

(19)日本国特許庁 (J P)

(12) 公 開 特 許 公 報 (A)

(11)特許出願公開番号
特開2001-216045
(P2001-216045A)

(43)公開日 平成13年 8月10日 (2001.8.10)

(51)Int.Cl. ⁷	識別記号	F I	テーマコード*(参考)
G 0 6 F 1/00	3 7 0	G 0 6 F 1/00	3 7 0 E 5 B 0 8 5
	3 3 0	15/00	3 3 0 F 5 J 1 0 4
H 0 4 L 9/32		H 0 4 L 9/00	6 7 3 D

審査請求 有 請求項の数14 O L (全 9 頁)

(21)出願番号 特願2000-25816(P2000-25816)

(22)出願日 平成12年 2月 3日 (2000.2.3)

(71)出願人 000004237

日本電気株式会社

東京都港区芝五丁目7番1号

(72)発明者 内田 薫

東京都港区芝五丁目7番1号 日本電気株式会社内

(74)代理人 100088812

弁理士 ▲柳▼川 信

Fターム(参考) 5B085 AE13 AE28 AE29

5J104 AA07 AA14 KA01 KA04 KA16

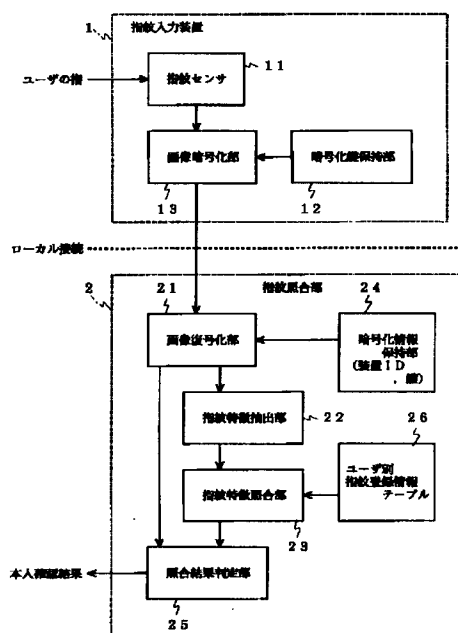
KA17 NA02

(54)【発明の名称】 バイオメトリクス入力装置及びバイオメトリクス照合装置

(57)【要約】

【課題】 バイオメトリクス入力部と処理部とが必ずしも一体化していない場合でもセキュリティホールを生じさせることなく、確実な本人確認を行うことが可能なバイオメトリクス入力装置を提供する。

【解決手段】 指紋センサ11は指が接触した際にその指紋画像を撮影し、撮影した入力画像をデジタルデータに変換してから画像暗号化部13に送る。画像暗号化部13は暗号化鍵保持部12から暗号化鍵を基に入力画像の暗号化処理を行う。画像復号化部21は暗号化情報保持部24からの鍵を用い、指紋入力装置1から受取った信号を復号する。指紋特徴抽出部22は復号された結果の画像情報から指紋照合に用いる特徴を計算する。指紋特徴照合部23は指紋特徴抽出部22で求められた指紋特徴とユーザ別指紋登録情報テーブル26に登録されているユーザの指紋特徴との照合を行い、結果を照合結果判定部25に渡す。



【特許請求の範囲】

【請求項1】 個人に固有の生体特徴であるバイオメトリクスをデジタル化するセンサ手段と、予め設定された秘密情報である暗号化鍵を保持する秘密情報保持手段と、前記センサ手段でデジタル化されたバイオメトリクスを前記秘密情報保持手段に保持された暗号化鍵に基づいて暗号化して出力するバイオメトリクス暗号化手段とを有することを特徴とするバイオメトリクス入力装置。

【請求項2】 前記センサ手段と前記秘密情報保持手段及び前記バイオメトリクス暗号化手段とを不可分な部分として構成するようにしたことを特徴とする請求項1記載のバイオメトリクス入力装置。

【請求項3】 前記バイオメトリクスとして指紋を用いるようにしたことを特徴とする請求項1または請求項2記載のバイオメトリクス入力装置。

【請求項4】 個人に固有の生体特徴であるバイオメトリクスをデジタル化するセンサ手段と、予め設定された秘密情報である暗号化鍵を保持する秘密情報保持手段と、前記センサ手段でデジタル化されたバイオメトリクスを前記秘密情報保持手段に保持された暗号化鍵を電子透かしとして埋め込む電子透かしエンコーダとを有することを特徴とするバイオメトリクス入力装置。

【請求項5】 前記センサ手段と前記秘密情報保持手段及び前記バイオメトリクス暗号化手段とを不可分な部分として構成するようにしたことを特徴とする請求項4記載のバイオメトリクス入力装置。

【請求項6】 前記バイオメトリクスとして指紋を用いるようにしたことを特徴とする請求項4または請求項5記載のバイオメトリクス入力装置。

【請求項7】 バイオメトリクス入力装置毎に予め設定された秘密情報である暗号化鍵を保持する保持手段と、前記暗号化鍵に基づいて暗号化されたバイオメトリクスの入力時に前記保持手段に保持された前記バイオメトリクス入力装置固有の暗号化鍵を用いて当該バイオメトリクスを復号化する復号化手段と、前記復号化手段で復号化された前記バイオメトリクスの照合処理を行う照合処理手段とを有することを特徴とするバイオメトリクス照合装置。

【請求項8】 前記バイオメトリクスとして指紋を用いるようにしたことを特徴とする請求項7記載のバイオメトリクス照合装置。

【請求項9】 バイオメトリクス入力装置毎に予め設定された秘密情報である暗号化鍵に基づいて暗号化されたバイオメトリクスの入力時に別途入手した前記バイオメトリクス入力装置固有の暗号化鍵を用いて当該バイオメトリクスを復号化する復号化手段と、前記復号化手段で復号化された前記バイオメトリクスの照合処理を行う照合処理手段とを有することを特徴とするバイオメトリクス照合装置。

【請求項10】 前記バイオメトリクスとして指紋を用いるようにしたことを特徴とする請求項9記載のバイオメトリクス照合装置。

【請求項11】 バイオメトリクス入力装置毎に予め設定された秘密情報である暗号化鍵を保持する保持手段と、前記暗号化鍵が電子透かしとして埋め込まれたバイオメトリクスの入力時に当該バイオメトリクスから前記暗号化鍵を取り出す手段と、その取り出された前記暗号化鍵と前記保持手段に保持された暗号化鍵とを比較して前記バイオメトリクス入力装置からの信号の正当性を判定する手段と、その判定結果を用いて前記バイオメトリクスの照合処理を行う照合処理手段とを有することを特徴とするバイオメトリクス照合装置。

【請求項12】 前記バイオメトリクスとして指紋を用いるようにしたことを特徴とする請求項11記載のバイオメトリクス照合装置。

【請求項13】 バイオメトリクス入力装置毎に予め設定された秘密情報である暗号化鍵が電子透かしとして埋め込まれたバイオメトリクスの入力時に当該バイオメトリクスから前記暗号化鍵を取り出す手段と、その取り出された前記暗号化鍵と別途入手した前記バイオメトリクス入力装置固有の秘密情報とを比較して前記バイオメトリクス入力装置からの信号の正当性を判定する手段と、その判定結果を用いて前記バイオメトリクスの照合処理を行う照合処理手段とを有することを特徴とするバイオメトリクス照合装置。

【請求項14】 前記バイオメトリクスとして指紋を用いるようにしたことを特徴とする請求項13記載のバイオメトリクス照合装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明はバイオメトリクス入力装置及びバイオメトリクス照合装置に関し、特に情報セキュリティ等におけるユーザ確認、個人識別のためのバイオメトリクス入力装置及びバイオメトリクス照合装置に関する。

【0002】

【従来の技術】情報の電子化やネットワークを通じての情報サービスにおいて、データの盗聴・改竄や「なりすまし」といった不正・犯罪に対抗するセキュリティの確保のためには、情報にアクセスする人間が正当な権限を持つユーザであるか、または価値の交換の相手が自分の望むユーザであるかを確認するための本人確認の実現が必須の条件となる。

【0003】現在、本人確認には磁気カードやパスワードが利用されているが、例えばカードをなくしたり、パスワードを忘れてしまうと本人でも使えないという不便さがあるのはもちろん、いずれの場合も盗難・偽造や盗み見・推量によって容易に他人がなりすませるといった問題点がある。

【0004】そこで、これらの問題点を解決するバイオメトリクスが用いられる。バイオメトリクスとは指紋のような個人に特有な生体特徴を利用するものである。人間の指先の皮膚紋様である指紋は「万人不同」・「終生不変」という特徴を持つとされ、表皮が損傷を受けてもその奥の不変な真皮から同じ指紋が復元されるため、精密な個人の同定を可能にするバイオメトリクスとして広く知られている。

【0005】バイオメトリクスによって個人を認証するシステムは基本的に、ユーザが提示したバイオメトリクスをシステム側で取得する「バイオメトリクス入力装置」と、入力されたデータを処理し照合に用いる特徴を求める「特徴抽出部」と、予め求めて記憶しておく正規ユーザについての登録データ（「テンプレート」）と、登録データと入力データ（の特徴同士）とを比較して同一人物であるか否かを決定する「照合・判定部」とから構成されている。

【0006】照合の結果、特徴が十分類似し、バイオメトリクスの提示者が登録ユーザであると判定されれば、認証成功ということで、認証要求者は要求するサービスを受けられる。以下、バイオメトリクスの例として指紋を挙げて説明する。

【0007】指紋の入力装置としては従来、光学方式、特に高コントラストな画像を得るためにプリズムでの全反射を利用する方法のみが用いられてきている。これはLED（Light Emitting Diode）光源で発した光をプリズムに当ててからCCD（Charge Coupled Device）のような受光素子で受け、プリズムの反射面に置いた指の凹凸を反射率の違いに反映させ、デジタル画像化するというものである。

【0008】また近年は、光学方式以外のセンシングを可能とする素子として、半導体チップの表面に直接接触させた指紋からその凹凸をセンスする、例えば静電容量方式のもの、温度や電界の差を検知する方式のもの等も実用化されつつある。

【0009】

【発明が解決しようとする課題】指紋照合処理の実現方法としては、入力装置が指紋の入力だけを行い、識別処理が接続されたPC（パーソナルコンピュータ）やネットワークで結ばれたサーバ等で行うという方法がとられることがある。

【0010】このように、指紋入力装置（スキャナ）と照合処理部とが分離している場合、入力装置（入力スキャナ、入力センサと呼ばれることもある）は指紋画像の入力を行い、それをケーブル等を通してPCに送り、そこで特徴抽出や照合・判定処理が実行される。

【0011】このような構成ではケーブルを付け替えて他の情報機器を結び、他の機会に入手した他人の指紋の画像データを、入力センサを装って照合処理部に入力す

るというセキュリティアタックがあり得る。この場合、照合処理部ではサービスを要求する本人の指紋と考えてサービスを許可するが、実際には他人の指紋であったということが起こりうる。

【0012】そこで、本発明の目的は上記の問題点を解消し、バイオメトリクス入力部と処理部とが必ずしも一体化していない場合でもセキュリティホールを生じさせることなく、確実な本人確認を行うことができるバイオメトリクス入力装置及びバイオメトリクス照合装置を提供することにある。

【0013】

【課題を解決するための手段】本発明によるバイオメトリクス入力装置は、個人に固有の生体特徴であるバイオメトリクスをデジタル化するセンサ手段と、予め設定された秘密情報である暗号化鍵を保持する秘密情報保持手段と、前記センサ手段でデジタル化されたバイオメトリクスを前記秘密情報保持手段に保持された暗号化鍵に基づいて暗号化して出力するバイオメトリクス暗号化手段とを備えている。

【0014】本発明による他のバイオメトリクス入力装置は、個人に固有の生体特徴であるバイオメトリクスをデジタル化するセンサ手段と、予め設定された秘密情報である暗号化鍵を保持する秘密情報保持手段と、前記センサ手段でデジタル化されたバイオメトリクスに前記秘密情報保持手段に保持された暗号化鍵を電子透かしとして埋め込む電子透かしエンコーダとを備えている。

【0015】本発明によるバイオメトリクス照合装置は、バイオメトリクス入力装置毎に予め設定された秘密情報である暗号化鍵を保持する保持手段と、前記暗号化鍵に基づいて暗号化されたバイオメトリクスの入力時に前記保持手段に保持された前記バイオメトリクス入力装置固有の暗号化鍵を用いて当該バイオメトリクスを復号化する復号化手段と、前記復号化手段で復号化された前記バイオメトリクスの照合処理を行う照合処理手段とを備えている。

【0016】本発明による他のバイオメトリクス照合装置は、バイオメトリクス入力装置毎に予め設定された秘密情報である暗号化鍵に基づいて暗号化されたバイオメトリクスの入力時に別途入手した前記バイオメトリクス入力装置固有の暗号化鍵を用いて当該バイオメトリクスを復号化する復号化手段と、前記復号化手段で復号化された前記バイオメトリクスの照合処理を行う照合処理手段とを備えている。

【0017】本発明による別のバイオメトリクス照合装置は、バイオメトリクス入力装置毎に予め設定された秘密情報である暗号化鍵を保持する保持手段と、前記暗号化鍵が電子透かしとして埋め込まれたバイオメトリクスの入力時に当該バイオメトリクスから前記暗号化鍵を取り出す手段と、その取り出された前記暗号化鍵と前記保持手段に保持された暗号化鍵とを比較して前記バイオメ

トリクス入力装置からの信号の正当性を判定する手段と、その判定結果を用いて前記バイオメトリクスの照合処理を行う照合処理手段とを備えている。

【0018】本発明によるさらに別のバイオメトリクス照合装置は、バイオメトリクス入力装置毎に予め設定された秘密情報である暗号化鍵が電子透かしとして埋め込まれたバイオメトリクスの入力時に当該バイオメトリクスから前記暗号化鍵を取り出す手段と、その取り出された前記暗号化鍵と別途入手した前記バイオメトリクス入力装置固有の秘密情報とを比較して前記バイオメトリクス入力装置からの信号の正当性を判定する手段と、その判定結果を用いて前記バイオメトリクスの照合処理を行う照合処理手段とを備えている。

【0019】すなわち、本発明のバイオメトリクス入力装置は、入力装置で取得されるバイオメトリクスデータを入力装置固有の鍵で暗号化し、あるいは入力装置固有のデータを電子透かしとして埋め込むことで、照合装置側でバイオメトリクス入力装置の正当性を確認可能とする。

【0020】これによって、バイオメトリクス入力装置が改造・置換され、あるいは出力信号が置換された場合にそれを検知することが可能となるので、バイオメトリクス入力部と処理部とが必ずしも一体化していない場合でもセキュリティホールを生じさせることなく、確実な本人確認を行うことが可能となる。

【0021】

【発明の実施の形態】次に、本発明の実施例について図面を参照して説明する。図1は本発明の一実施例によるバイオメトリクス入力装置の構成を示すブロック図である。図1においてはPC等においてユーザのログインを指紋で行う場合の構成の一例を示しており、指紋入力装置1をケーブル等のローカルな接続によってPCに接続し、PC上のソフトウェアで指紋照合部2が動作するようになっている。

【0022】指紋入力装置1には指紋センサ11が装備されており、指紋センサ11はユーザの指が接触した際にその指紋画像を撮影し、撮影した入力画像をデジタルデータに変換してから画像暗号化部13に送る。暗号化鍵保持部12は一般ユーザ等に知られていない秘密情報としてその指紋入力装置1の個体固有の暗号化鍵を保持する。これは、例えば256ビットのビット列等である。

【0023】画像暗号化部13は暗号化鍵保持部12からその暗号化鍵を受取り、これを鍵として入力画像の暗号化処理を行う。この暗号化処理としては、DES(Data Encryption Standard)を例とするような共通秘密鍵方式の暗号化方法を用いることができるが、また一方、RSA方式を例とするような公開鍵方式(非対称暗号系)の暗号化方式を利用することも可能である。この場合、指紋入力装置1の持つ秘密鍵

を暗号化に用いることになる。

【0024】また、用途によっては複雑な暗号化処理でなくとも、入力画像のラインや画素毎にシフトしたり、入れ替えたりするスクランブル処理を採用し、そのスクランブルを規定するルールを暗号化鍵として暗号化鍵保持部12に置くという方法も可能である。

【0025】一方、指紋入力装置1の構成法としては、指紋センサ11、画像暗号化部13、暗号化鍵保持部12を不可分な方法で構成することが望ましい。不可分であるとは、ここの部分の解読や改造を図る不当な第三者が、指紋センサ11から画像暗号化部13への内部信号、暗号化鍵保持部12から画像暗号化部13への内部信号を解読したり、それらの信号を外部からの信号で置き換えたり、あるいはそれぞれの構成要素の中身を解読したり改造したりできないように構成するということである。

【0026】この実現法としては、指紋センサ11の画像取得及びデジタル化を実行する半導体チップと同一チップ上に画像暗号化部13と暗号化鍵保持部12とを焼き込むという方法が有効である。一例としては、指紋センサ11の撮像部としてCMOS(Complementary Metal Oxide Semiconductor)のイメージチップを利用し、その同一チップ上で暗号鍵の保持から暗号化演算までを行い、暗号化した結果を出力信号とするという実装があり得る。

【0027】あるいは、指紋センサ11の指紋画像取得方法として半導体センサによる静電容量方式の指紋センシングを利用し、その半導体センサ上に暗号鍵の保持から暗号化演算までを実装するということもできる。

【0028】指紋入力装置1とケーブル等のローカルな接続によって結ばれた指紋照合部2ではその内部の暗号化情報保持部24に、その指紋照合部2が接続して使用する指紋入力装置1の個体毎に固有な暗号化鍵を、その入力装置の識別子(装置ID)と対して記憶しておき、現在接続されているはずの指紋入力装置1の装置IDに対応する鍵を指紋復号化部21に渡す。画像復号化部21はその鍵を用い、指紋入力装置1から受取った信号を復号する。

【0029】この復号処理は指紋入力装置1の画像暗号化部13の処理内容に対応したものをを用い、正しく意味ある信号が復元できることをもって、指紋入力装置1及びそこから送られてくる信号の正当性を確認することとなる。

【0030】例えば、画像暗号化部13が共通秘密鍵方式の暗号化方法を用いていれば、暗号化鍵保持部12に保持されたものと同一の鍵を用いた復号を行い、これで正しく復号できる場合には指紋入力装置1及びそこから送られてくる信号が正当なものであることを確認することができる。

【0031】また、公開鍵方式(非対称暗号系)の暗号

化方式であれば、指紋入力装置1の暗号化鍵保持部12に保持された秘密鍵に対応する公開鍵を用いて復号する。これで正しく復号できる場合には指紋入力装置1及びそこから送られてくる信号が正当なものであることを確認することができる。

【0032】さらに、画像暗号化部13が入力画像のラインや画素毎にシフトしたり、入れ替えたりするスクランブル処理を用いた場合にも、暗号化鍵保持部12が持っているはずのスクランブルを規定するルールを鍵として暗号化情報保持部24に保持しておき、それを用いて対応する復号化を行う。これで正しく復号できる場合には指紋入力装置1及びそこから送られてくる信号が正当なものであることを確認することができる。

【0033】指紋特徴抽出部22は画像復号化部21で復号された結果の画像情報から指紋照合に用いる特徴を計算する。ユーザ別指紋登録情報テーブル26は指紋照合に用いる指紋特徴情報をユーザ毎に保持している。指紋特徴照合部23は指紋特徴抽出部22で求められた指紋特徴とユーザ別指紋登録情報テーブル26に登録されているユーザの指紋特徴との照合を行い、結果を照合結果判定部25に渡す。

【0034】以上の指紋センサ11、指紋特徴抽出部22、指紋特徴照合部23を含む指紋照合装置の実現例としては、特開昭56-24675号公報や特開平4-33065号公報に記載された「指紋照合装置」がある。

【0035】特開昭56-24675号公報に記載された「指紋照合装置」では、指紋等の照合に際して、指紋紋様を特徴付ける各特徴点の位置X、Y及び方向Dとともに各特徴点により固有に決定される局所座標系を複数個の扇形領域に分割した近傍における最近傍点と上記特徴点との隆線数、すなわちリレーションを検査することによって、安定で、かつ精度の高い照合を可能にしている。

【0036】また、特開平4-33065号公報に記載された「指紋照合装置」では、登録されている一つの指もしくは複数の指の全てと入力指紋との照合を行うことによって、暗証番号の盗難や忘却に関与しない、操作性が優れかつ信頼性の高い同定を可能としている。

【0037】照合結果判定部25は指紋入力装置1から送られてくる信号の正当性と、指紋特徴照合部23で求められる指紋照合の結果とを総合し、本人確認の結果として出力する。先に述べたように、指紋照合部2は使用されているはずの指紋入力装置1に固有で秘密であるはずの鍵情報を暗号化情報保持部24のテーブルから探索し、それを用いて指紋入力装置1から送られる信号を復号し、それが正しく意味ある信号であるか否かを確認する。

【0038】正しく意味ある信号とはすなわち、指紋入力装置1において指紋センサ11から出力された信号の形式に合致していることを意味し、これが合致している

場合には指紋入力装置1が正当なもので、また指紋入力装置1からの信号は途中で改変されていないことが確認できたとして、指紋照合結果は信頼できるものであると判断する。

【0039】一方、合致していない等、正しく復号できなかった場合には、それは指紋入力装置1が正当なものではないか、または指紋入力装置1からの信号が途中で改変されたことを意味するので、指紋照合結果は信頼できるものではないと判断することになる。

【0040】図2は本発明の他の実施例による画像入力装置の構成を示すブロック図である。図2においては本発明の一実施例と同様に、PC等においてユーザのログインを指紋で行う場合の構成の一例を示しており、指紋入力装置3をケーブル等のローカルな接続によってPCに接続し、PC上のソフトウェアで指紋照合部4が動作する。

【0041】指紋入力装置3には指紋センサ11が装備されており、指紋センサ11はユーザの指が接触した際にその指紋画像を撮影し、撮影した入力画像をデジタルデータに変換してから電子透かしエンコーダ31に送る。指紋入力装置秘密情報保持部33は一般ユーザ等に知られていない秘密情報としてその指紋入力装置3の個体固有の秘密情報を保持する。これは、例えばパスワードのような文字列等である。

【0042】電子透かしエンコーダ31は指紋入力装置秘密情報保持部33からその秘密情報を受取り、電子透かしエンコード方式によってこれを入力画像に埋め込む。電子透かし技術とは次のような特徴を持つ。

【0043】すなわち、(1)透かしデータをコンテンツの中に、不可視の状態で埋め込むことができる、

(2)透かしの埋め込んだ者が必要な時に抽出することが可能である、(3)透かしはコンテンツを加工しても残り、抽出が可能である、(4)コンテンツの利用価値を保ったまま第三者が電子透かしを除去するのは困難であるという特徴を持つ。(2)は暗号化技術におけるキーのような情報を設定し、キーを用いなければ情報が取り出せないような仕組みを設けることによって行われる。

【0044】上記の電子透かし技術を使用することによって、コンテンツである指紋画像を劣化させることなく、電子透かしデータをその中に埋め込むことができ、そのデータを秘密に保つことができる。また、指紋画像を大幅に劣化させることなく、透かしデータを分離・削除・改変することもできない。電子透かし技術の実現法の例としては、例えば特開平8-241403号公報に記載の方法や特開平10-2247933号公報に記載の技術等がある。

【0045】特開平8-241403号公報に記載の方法では、ウォーターマーク画像の画素を検査し、その値が指定された「透明」値でない画素のそれぞれについ

て、現画像の対応する画素を、その色度ではなく輝度を変更することによって修正することで、画像の内容を明瞭に見ることができるが、画像の無認可使用をおもいとどまらせる可視のマークをもたすようにしている。

【0046】また、特開平10-2247933号公報に記載の技術では、電子透かしが挿入されたMPEG (Moving Picture Expert Group) ストリームとともに、挿入された電子透かしデータも出力することで、挿入する電子透かしデータの管理を簡単にしている。

【0047】尚、上記の指紋入力装置3の構成法としては、本発明の一実施例と同様に、指紋センサ11、指紋入力装置秘密情報保持部33、電子透かしエンコーダ31を不可分な方法で構成することが望ましい。また、電子透かしエンコーダ31の出力信号はこのままユーザの指紋画像データが見える形で含むので、通信内容秘匿のために暗号部32において暗号化処理を行う。これは通常よく使われるDESの秘密共通鍵方式等の暗号化方式でよく、以下に述べる復号部41と鍵情報を共用していればよい。

【0048】指紋入力装置3とケーブル等のローカルな接続によって結ばれた指紋照合部4においては、まず復号部41において通信内容秘匿のための暗号化を解き、電子透かしエンコーダ31の出力信号を復元する。その後、電子透かしデコーダ42において、電子透かしエンコーダ31のエンコードの方法に対応したデコード(復号化)処理を行い、指紋画像信号からそこに埋め込まれた透かしデータを分離して検出する。

【0049】指紋入力装置3は指紋画像信号とは別に、その装置固有のID(識別子)を指紋照合部4に送る。指紋照合部4ではその内部の指紋入力装置ID保持部43に、その指紋照合部4が接続して使用する指紋入力装置3の個体に対応する秘密情報をその入力装置の識別子(装置ID)と対して記憶しておく。この秘密情報は該当指紋入力装置の指紋入力装置秘密情報保持部33に保持されている情報と同一のものである。

【0050】指紋入力装置ID保持部43は指紋入力装置3から受取ったIDでこのテーブルをひき、対応する秘密情報を読み出して指紋入力装置ID比較部44に渡す。指紋入力装置ID比較部44はその値と、電子透かしデコーダ42において検出された透かしデータとを比較する。もしも、指紋入力装置3が正当なものであればこれらは一致するはずであり、そうでなければ不一致となる。

【0051】指紋特徴抽出部22は電子透かしデコーダ42から出力された画像情報から指紋照合に用いる特徴を計算する。ユーザ別指紋登録情報テーブル26は指紋照合に用いる指紋特徴情報をユーザ毎に保持しているものである。指紋特徴照合部23は指紋特徴抽出部22で求められた指紋特徴とユーザ別指紋登録情報テーブル2

6に登録された指紋特徴との照合を行い、結果を照合結果判定部25に渡す。

【0052】照合結果判定部25は指紋入力装置ID比較部44が判定する指紋入力装置3の正当性と、指紋特徴照合部23で求められる指紋照合の結果とを総合し、本人確認の結果として出力する。先に述べたように、指紋照合部4は使用されているはずの指紋入力装置3に固有で秘密であるはずの情報が電子透かしとして埋め込まれていれば、指紋入力装置3が正当なもので、また指紋入力装置3からの信号が途中で改変されていないことを確認することができたとして、指紋照合結果を信頼できるものであると判断する。

【0053】そうでない場合には、それは指紋入力装置3が正当なものではないか、または指紋入力装置3からの信号が途中で改変されたことを意味するので、指紋照合結果を信頼できるものではないと判断することになる。

【0054】図3は本発明の別の実施例による画像入力装置の構成を示すブロック図である。図3においては本発明の他の実施例による画像入力装置をネットワークで結ばれた指紋照合に拡張したものである。

【0055】指紋入力装置5はユーザが利用するサービスクライアント7に接続されている。これは例えばユーザのオフィスの机の上にあるPC、ユーザの家庭にあるPC、あるいは店舗の店頭等にある公衆向けのPOS(Point Of Sales)端末でもよい。これらのサービスクライアントは顧客であるユーザに対してさまざまな情報サービスや電子商取引の提供端末として働くが、ユーザの本人確認・認証に関しては指紋サーバ6と指紋入力装置5との通信を、中身を変えずに橋渡しする透明な仲介者として機能する。

【0056】サービスクライアント7に接続された指紋入力装置5は本発明の他の実施例と同様の構成を持ち、同様の動作を行う。電子透かしが埋め込まれた指紋入力画像はサービスクライアント7を通過して指紋サーバ6に送られる。

【0057】サービスクライアント7とネットワークによって結ばれた指紋サーバ6は基本的に本発明の他の実施例と同様の構成を持ち、同様の動作を行う。すなわち、電子透かしを検出し、これによって判定される指紋入力装置5の正当性と、指紋特徴照合部23で求められる指紋照合の結果とを総合し、本人確認の結果として出力する。

【0058】但し、指紋入力装置5は、本発明の他の実施例の場合と異なり、指紋画像信号とは別に指紋入力装置秘密情報保持部33に保持された秘密情報を、公開鍵暗号部51が指紋サーバ6に対応するRSA方式の公開鍵を用いて暗号化して指紋サーバ6に送る。

【0059】秘密鍵復号部61では送られてきた信号を自分の公開鍵に対応した秘密鍵によって復号し、指紋入

力装置 I D 比較部 4 4 での比較に用いる。指紋サーバ 6 に対応する R S A 方式の公開鍵を用いて暗号化された秘密情報は、その公開鍵に対応した秘密鍵によってのみ復号可能である。

【0060】この部分については本発明の他の実施例に準じて、ネットワーク内に結ばれた全ての指紋入力装置 5 に対応する秘密情報と指紋入力装置 5 との対を予め指紋サーバ 6 がその内部に保持しておくという実現法もちろん可能ではあるが、指紋入力装置 5 の数が多くなり、また変更・交換等に対応するためには、このように別のチャンネルで直接秘密情報を送る方が優れているといえる。

【0061】指紋サーバ 6 は照合結果判定部 2 5 の出力をサービスクライアント 7 に知らせ、指紋を入力したユーザが正規のユーザでありかつ指紋入力装置 5 が正規の装置であると判定の結果から確認できた時に限り、サービスクライアント 7 はユーザの要求するサービスをそのユーザに対して提供する。

【0062】上記の本発明の実施例の説明では、バイOMETRICS の一例として指紋の場合を挙げて説明しているが、指紋センサ 1 1 と、指紋特徴抽出部 2 2、指紋特徴照合部 2 3 の部分を別のバイOMETRICS を入力し、特徴を抽出して照合する手段で置換すれば、掌紋、顔、虹彩、網膜血管パターン、掌形、筆跡、声紋等の他のバイOMETRICS を使用することも可能である。例えば、声紋の場合にはマイクで入力され、デジタル化された後の音声データに対してマイクと不可分な装置で暗号化や電子透かしの埋め込みを施すことで、入力部の正当性を確認することができる。

【0063】このように、照合装置以外は解読できない信号、あるいはその中に埋め込まれた電子透かしを解読し、また改変できない信号をバイOMETRICS 入力装置と照合装置との間での通信に用いることによって、バイOMETRICS 入力装置が改造、置換されず正当なものであることを判定して本人認証を実行することができる。

【0064】これによって、バイOMETRICS 入力装置が照合装置とケーブルやネットワーク等で接続され、分離している場合でも、ケーブルを付け替えて他の情報機器を結び、他の機会に入手した他人の指紋の画像データを、入力センサを装って照合処理部に入力するという種類のセキュリティアタックを防ぐことができる。つまり、照合処理部ではサービスを要求する本人の指紋と考えてサービスを許可するが、実際は他人の指紋であったということは起こり得ない。

【0065】すなわち、データが登録されていない不適合スキャナからの指紋データで置き換えられた場合、データの一部に操作が加えられた場合、一部が失われた場

合にはそれらを検知し、認証結果に反映させることができる。

【0066】また、本発明の別の実施例の構成をとることによって、ネットワーク上に多数のバイOMETRICS 入力装置がある場合にも、それぞれが正当なものであることを確認しながらユーザ認証を実現することができる。

【0067】

【発明の効果】以上説明したように本発明によれば、個人に固有の生体特徴であるバイOMETRICS をデジタル化し、そのデジタル化したバイOMETRICS を予め設定された秘密情報である暗号化鍵に基づいて暗号化して出力することによって、バイOMETRICS 入力部と処理部とが必ずしも一体化していない場合でもセキュリティホールを生じさせることなく、確実な本人確認を行うことができるという効果がある。

【図面の簡単な説明】

【図 1】本発明の一実施例によるバイOMETRICS 入力装置の構成を示すブロック図である。

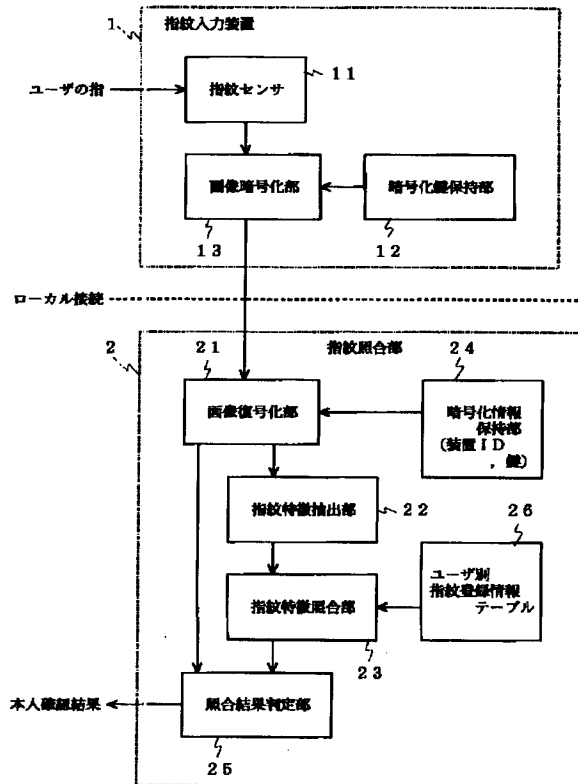
【図 2】本発明の他の実施例によるバイOMETRICS 入力装置の構成を示すブロック図である。

【図 3】本発明の別の実施例によるバイOMETRICS 入力装置の構成を示すブロック図である。

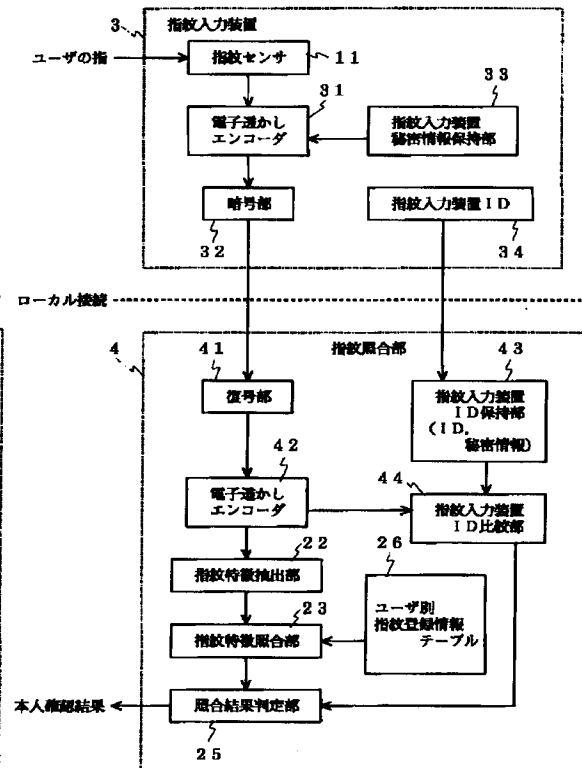
【符号の説明】

- 1, 3, 5 指紋入力装置
- 2, 4 指紋照合部
- 6 指紋サーバ
- 7 サービスクライアント
- 11 指紋センサ
- 12 暗号化鍵保持部
- 13 画像暗号化部
- 21 画像復号化部
- 22 指紋特徴抽出部
- 23 指紋特徴照合部
- 24 暗号化情報保持部
- 25 照合結果判定部
- 26 ユーザ別指紋登録情報テーブル
- 31 電子透かしエンコーダ
- 32 暗号部
- 33 指紋入力装置秘密情報保持部
- 41 復号部
- 42 電子透かしデコーダ
- 43 指紋入力装置 I D 保持部
- 44 指紋入力装置 I D 比較部
- 51 公開鍵暗号部
- 61 秘密鍵復号部

【図1】



【図2】



【図3】

